Exhibit 1

for

United States' Rebuttal Expert Disclosure

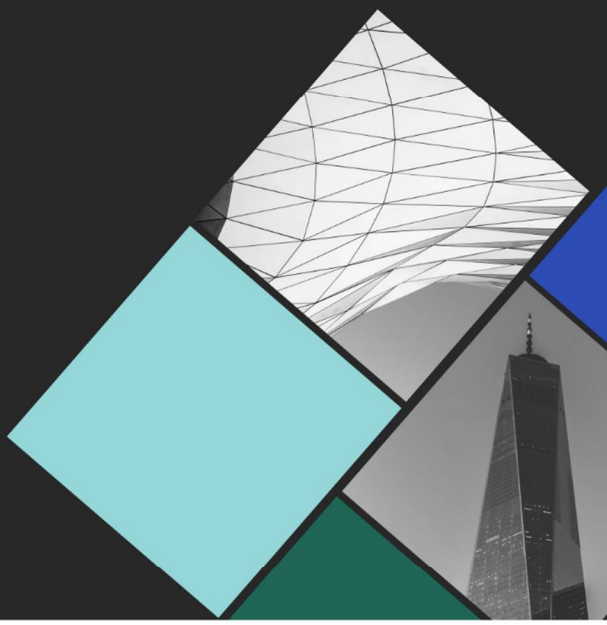
Curriculum Vitae for

Matthew J. Edman, Ph.D.

Computer Scientist

CURRICULUM VITAE

Matthew J. Edman, Ph.D.



NAXO

Matthew J. Edman, Ph.D.

PARTNER & CO-FOUNDER
NAXO

45 Rockefeller Plaza, Suite 1964, New York, NY 10111
matt@naxo.com | www.naxo.com

Matthew J. Edman, Ph.D., is a computer scientist specializing in cybersecurity and crypto asset investigations. His areas of expertise include blockchain analysis, cybersecurity, and digital forensic investigations; network security, penetration testing, and vulnerability assessments; secure software development and source code audits; forensic analysis, reverse engineering, and software exploitation. Dr. Edman also provides expert testimony on matters related to cryptocurrency, cybersecurity, and digital forensic investigations.

Dr. Edman previously worked as a lead cybersecurity engineer for a federally funded research and development center, where he provided specialized computer and network security research and development to federal law enforcement. Leading an interdisciplinary team of researchers, he developed a groundbreaking network-investigative technique that has successfully provided critical intelligence in multiple high-profile law enforcement investigations related to darknet markets.

Prior to co-founding NAXO, Dr. Edman worked as a senior vulnerability engineer for a global financial services, software, and media company based in New York. As a member of the firm's vulnerability analysis team, his work helped protect sensitive client data from both internal and external threats through continuous research and penetration testing of the firm's entire technological infrastructure.

Dr. Edman holds a B.S. in Computer Science from Baylor University, and an M.S. and Ph.D. in Computer Science from Rensselaer Polytechnic Institute, where his research areas included novel techniques for cryptographic security and authentication in wireless networks, and the design, implementation, and analysis of anonymous communication systems on the Internet.

He has published scientific articles in peer-reviewed conferences and journals and has served as an invited program committee member for the ACM Conference on Computer and Communications Security and the IFCA International Conference on Financial Cryptography and Data Security. Dr. Edman has also served as an external reviewer for several academic conferences and journals, including IET Information Security and the Privacy Enhancing Technologies Symposium.

EDUCATION

PH.D., COMPUTER SCIENCE
Rensselaer Polytechnic Institute, 2011

M.S., COMPUTER SCIENCE
Rensselaer Polytechnic Institute, 2007

B.S., COMPUTER SCIENCE
Baylor University, 2005

CERTIFICATIONS

AccessData Certified Examiner

Chainalysis Investigative Specialist Certification

Chainalysis Ethereum Investigations Certification

Chainalysis Reactor Certification

PRIOR EXPERIENCE

BERKELEY RESEARCH GROUP New York, NY
Director, Cyber Operations & Incident Response
December 2015 – June 2022

- Co-created and developed BRG's Cyber Operations & Incident Response practice focused on responding to cyber security incidents for clients including financial institutions, cryptocurrency hedge funds and custodians, and private individuals.
- Spearheaded the establishment of BRG's blockchain and cryptocurrency practice area combining our investigative experience with experts in forensic accounting, e-discovery, and regulatory enforcement.
- Retained as an expert in a variety of civil and criminal matters related to cryptocurrency and cybersecurity.

FTI CONSULTING New York, NY
Senior Director, Cyber Security & Investigations
June 2014 – December 2015

- Contributed to a variety of computer and network forensic investigations and vulnerability assessments as a member of FTI's Cyber Security & Investigations Group.
- Performed forensic evidence collection and analysis in response to breaches of client systems and networks by external threats or theft of proprietary information by corporate insiders, as well as proactive penetration testing and vulnerability assessments of client networks.
- Retained as an expert witness in multiple civil litigations, including developing custom tools for analyzing proprietary systems and datasets, preparing expert reports, and testifying in a deposition.

BLOOMBERG LP New York, NY
Senior Vulnerability Engineer, Information Security Group
July 2013 – June 2014

- Performed source code reviews, penetration testing, and "red team" vulnerability assessments of internal and third-party applications, networks, and websites as a member of Bloomberg's Vulnerability Assessment Team.
- Developed custom tools for analyzing Bloomberg's proprietary network protocols and systems for vulnerabilities, as well as proof-of-concept exploits to demonstrate identified vulnerabilities.
- Participated in software and network design reviews to ensure new projects adhered to Bloomberg's security standards and best practices for design, development, implementation, and monitoring.

THE MITRE CORPORATION McLean, VA
Lead Cyber Security Engineer, Domestic Security Division
September 2009 – June 2013

- Provided on-site computer security research and engineering support to federal law enforcement agencies.
- Proposed and led an interdisciplinary research project involving subject-matter experts in signal processing and applied mathematics, which resulted in a novel investigative technique that provided crucial intelligence in multiple high-profile investigations.
- Nominated for a MITRE Technical Leadership Award for outstanding research accomplishments.

EXPERT TESTIMONY

- **Securities and Exchange Commission** v. Terraform Labs Pte. Ltd. and Do Hyeong Kwon, United States District Court for the Southern District of New York, 1:23:cv-01346-JSR. Expert report, deposition testimony, and trial testimony regarding analysis of source code and Terra blockchain activity allegedly associated with a Korean mobile payment application, Chai, which defendants claimed used the Terra blockchain to process and settle customer transactions in cryptocurrencies.

- United States of America v. **Nathaniel Chastain**, United States District Court for the Southern District of New York, 1:22-cr-00305-JMF. Expert analysis and trial testimony regarding cryptocurrency transactions and other records associated with the defendant's non-fungible token (NFT) trading activity on the OpenSea marketplace.

- **Kramer et al.** v. Coinbase, Inc. and Coinbase Global, Inc., Superior Court of California, County of San Francisco, CGC-23-604357. Expert declaration regarding an analysis of Coinbase's cybersecurity measures and other technical controls in connection with multiple alleged thefts of crypto assets from Coinbase users' exchange accounts.

- **Mark Owen et al.** v. Elastos Foundation, Feng Han, and Rong Chen, United States District Court for the Southern District of New York, 1:19-cv-5462-GHW. Expert declaration regarding certain crypto-assets and associated "initial coin offerings" and an analysis of geographic distribution of nodes in a blockchain network.

- **Chase Williams et al.** v. KuCoin, Michael Gan, Johnny Lyu, and Eric Don, United States District Court for the Southern District of New York, 1:20-cv-02806-GBD-RWL. Expert declaration regarding certain crypto-assets and an analysis of price history and trading volume associated with the tokens on a particular exchange.

- **Ira Kleiman, as the personal representative of the Estate of David Kleiman, and W&K Info Defense Research, LLC** v. Craig Wright, United States District Court for the Southern District of Florida, 9:18-cv-80176-BB. Affidavit, expert report, deposition testimony, evidentiary hearing testimony, and trial testimony regarding a forensic analysis of emails, PDFs, and other documents related to a disputed ownership of certain intellectual property and crypto assets. Expert analysis also included a review of IP address history and geolocation, domain registration records, and cryptocurrency addresses.

- **Rosebank Road Medical Services Ltd. d/b/a Rosebank Road Medical Centre and Geeta Murali Ganesh** v. Ramji Govindarajan and John Does 2-20, Superior Court of California, County of San Francisco, CGC-16-549755. Deposition and trial testimony regarding an investigation of certain alleged defamatory postings anonymously posted online and emailed to a government regulatory agency. Expert analysis also included a review of IP address history and geolocation, VPNs and other anonymous communication systems, email records, and web server logs.

- United States of America v. **Timothy Livingston a/k/a "Mark Lloyd,"** United States District Court for the District of New Jersey, Criminal No. 15-626 (WJM). Expert declarations regarding a forensic analysis of emails, email addresses, and other artifacts associated with an alleged computer intrusion. Expert analysis also included a review of IP address history, domain registration records, and website access control mechanisms.

- **Spanski Enterprises, Inc.** v. Telewizja Polska, S.A., United States District Court for the District of Columbia, 12-CV-957-TSC. Expert report, deposition, and trial testimony regarding an analysis of IP address history and geolocation, WHOIS records, and website "geoblocking" techniques related to an online TV streaming service.

PUBLICATIONS

- On the Security of Key Extraction from Measuring Physical Quantities (with Aggelos Kiayias, Qiang Tang, and Bülent Yener), IEEE Transactions on Information Forensics and Security (Volume 11, Issue 8), 2016.
- On Passive Inference Attacks Against Physical-layer Key Extraction (with Aggelos Kiayias and Bülent Yener), Proceedings of the 2011 European Workshop on System Security (EuroSec), 2011.
- On Anonymity in an Electronic Society: A Survey of Anonymous Communication Systems (with Bülent Yener), ACM Computing Surveys 42(1), 2009.
- AS-awareness in Tor Path Selection (with Paul Syverson), Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2009.
- Vidalia: Towards a Usable Tor GUI (with Justin Hipple), Proceedings of the Symposium on Usable Privacy and Security (SOUPS), 2007.
- A Combinatorial Approach to Measuring Anonymity (with Fikret Sivrikaya and Bülent Yener), Proceedings of the IEEE International Conference on Intelligence and Security Informatics (ISI), 2007.

PROFESSIONAL AFFILIATIONS

- **Member**, Association for Computing Machinery (ACM)
- **Member**, Institute of Electrical and Electronics Engineers (IEEE)
- **Member**, International Association for Cryptologic Research (IACR)
- **Cyber Security & Privacy Industry Advisory Board**
  New Jersey Institute of Technology
- **Program Committee**
  IFCA Conference on Financial Cryptography and Data Security, 2009
- **Program Committee**
  ACM Conference on Computer and Communications Security, 2007-2009

REPRESENTATIVE MATTERS

BLOCKCHAIN & CRYPTO ASSET INVESTIGATIONS

- Retained by counsel for a blockchain security auditing firm in connection with an internal investigation into allegations of unauthorized transactions related to a third-party crypto asset exchange's bug bounty program. Conducted crypto asset tracing and assisted counsel with investigating and responding to regulatory inquiries regarding alleged transactions involving OFAC-sanctioned smart contracts.
- Provided expert testimony in an arbitration regarding alleged deficiencies in a crypto asset exchange's DeFi wallet application which purportedly led to hundreds of users suffering losses totaling over $30 million from interactions with malicious distributed applications (or "dApps"). Analyzed smart contracts and blockchain transactions associated with the alleged thefts, internal communications related to development of the DeFi wallet application, and historical records from commonly used wallet attribution and compliance resources.

BLOCKCHAIN & CRYPTO ASSET INVESTIGATIONS (CONT'D)

- Retained by counsel for the Litigation Administrator in connection with bankruptcy proceedings of a multi-billion-dollar crypto asset exchange. Analyzed exchange database records related to deposits and withdrawals of crypto assets and traced certain crypto asset withdrawals to third-party exchanges in support of asset recovery efforts.

- Retained on behalf of a Fortune 500 telecommunications provider to provide expert analysis and testimony in an arbitration related to a purported theft of crypto assets which allegedly resulted from the telecommunications provider's negligent user authentication practices. Reviewed the provider's authentication policies and procedures, blockchain transactions associated with the alleged theft, and provided an expert report and testimony regarding industry standards and best practices for user identification and authentication and secure crypto asset storage.

- Retained by counsel for a blockchain-enabled ESG company to investigate a theft of the company's crypto assets. Conducted a forensic investigation into the source of the breach, an analysis of on-chain activity associated with theft to identify where the company's crypto assets were transferred and supported a referral to law enforcement which resulted in freezing the stolen funds.

- Provided expert testimony in an arbitration regarding industry standards and best practices for secure storage, backups, and disaster recovery of cryptocurrency keys, wallets, and seed phrases. Analyzed security policies and procedures of a cryptocurrency-focused hedge fund and compared them to general information security standards, including NIST SP 800-53 and ISO 27001:2013, as well as cryptocurrency-specific standards such as the Cryptocurrency Security Standard.

- Provided technical consulting to the US government related to the investigation of Silk Road, a $1.2 billion illicit drug market hosted on the dark web. Worked on-scene with US and international law enforcement to affect the seizure of over 170,000 bitcoins stored on the market's web servers and other devices belonging to its owner and operator, Ross Ulbricht.

- Investigated the theft of private keys controlling the minting of a cryptocurrency token. The stolen private keys were later used to mint one billion new tokens which, in turn, were then used to drain funds from a liquidity pool. Analyzed the cryptocurrency transactions associated with the funds drained from the liquidity pool and drafted a memorandum in support of a referral to law enforcement.

- Retained by plaintiffs in a civil suit regarding ownership of over $10 billion worth of bitcoins (at present valuation). Conducted a forensic analysis of numerous cryptocurrency-related documents and other forensic evidence related to alleged ownership and transfer of disputed bitcoins and provided expert analysis and testimony regarding alleged associated Bitcoin blockchain addresses, transactions, and related documents.

- Retained as an expert by plaintiffs in a class action lawsuit against a cryptocurrency exchange alleging, among other things, that the exchange promoted, offered, and sold unlicensed securities in the form of certain ERC-20 tokens. Provided written testimony to the court regarding ERC-20 tokens and conducted an analysis of the cryptocurrency exchange activity with respect to those tokens.

- Retained by counsel for a defendant in a criminal matter to analyze database records and blockchain transactions associated with an allegedly fraudulent cryptocurrency mining scheme valued at over $700 million.

- Retained by owners of a US-based mining operation to review historical mining activities, evaluate their deployed mining hardware and anticipated hardware upgrades, and estimate, to the extent possible, their expected mining rewards in the context of the 2020 Bitcoin halving event and anticipated mining difficulty adjustments.

BLOCKCHAIN & CRYPTO ASSET INVESTIGATIONS (CONT'D)

- Retained in a civil matter related to a dispute over the valuation of certain jointly held crypto wallets. Reviewed historical activity associated with the crypto assets at issue, derived valuations of those assets at various points in time based on publicly available pricing data and produced a report summarizing my methodology and findings.

- Conducted an independent analysis of token issuances, revocations, and other transaction activity for a virtual currency exchange that offers a "stable coin." Compared the blockchain activity with financial records and other documentation to evaluate the extent to which the tokens were backed by government-issued currency over a disputed period of time.

- Retained by counsel for plaintiffs in a matter alleging that the defendant—the owner and operator of a defunct Bitcoin exchange—failed to provide the full number of bitcoins in exchange for funds that the plaintiffs had invested in the exchange. Reviewed financial records in combination with blockchain transactions to determine the total amount of USD invested by the plaintiffs and bitcoins sent in return.

- Retained by counsel for the operators of an adult-oriented website who alleged that its users were being extorted by anonymous individuals demanding payment in bitcoins. Traced the blockchain transactions associated with the alleged extortion payments and identified the cryptocurrency exchange through which the Bitcoin payments were converted to fiat currency and provided additional investigative options to counsel for the client.

- Retained by the U.S. Attorney's Office for the Southern District of New York related to the prosecution of an individual accused of operating an unlicensed Bitcoin exchange. Analyzed forensic evidence collected by US law enforcement, recovered and analyzed encrypted database files related to Bitcoin and fiat currency transactions, and drafted summary exhibits regarding my findings.

- Retained by the U.S. Attorney's Office for the Southern District of New York related to the prosecution of an individual accused of operating a virtual currency exchange to facilitate a money laundering enterprise. Analyzed multiple databases containing over five million users and over 210 million transactions, representing a total transaction volume of over $16 billion USD.

- Retained by the U.S. Attorney's Office for the Southern District of New York to perform an analysis of the various Bitcoin wallets seized from Silk Road and from Ross Ulbricht's personal laptop, and to establish substantial and ongoing links between the two. Developed trial exhibits to support the successful prosecution of Ulbricht.

- Routinely hired to assist clients in recovering cryptocurrency wallets from theft, lost or forgotten passwords, or inadvertently deleted wallet data.

CYBERSECURITY

- Provided strategic consulting to a New York-based hedge fund regarding the secure storage and management of cryptocurrencies on behalf of its clients, as well as a strategic overview of its information security program in conjunction with its application for a "BitLicense" from the New York Department of Financial Services.

- Retained as an expert by a global marketing agency to review the design, development, testing, and deployment of a website intended to allow customers of an international computer and peripheral manufacturer to recycle printer cartridges. Evaluated claims that the website's security measures were insufficient and did not follow industry standards and best practices to mitigate abuse of the website.

CYBERSECURITY (CONT'D)

- Retained by a US-based pharmaceuticals company to conduct an evaluation of their information security program following a spear phishing attack that resulted in the compromise of an executive's email account. Conducted a review of the company's IT infrastructure, policies and procedures. Provided recommendations for improving security posture and drafted an incident response plan and procedure for the company.

- Retained as an expert in a bid protest on behalf of a defense contractor alleging a competitor's proposal violated numerous government security standards. Conducted reverse engineering and technical analysis of the hardware implementation proposed by the competitor. Evaluated the security of the device in the context of several government security and privacy standards, including NIST SP 800-53, FIPS 201, and FISMA.

- Retained by an international surgical device manufacturer to conduct an evaluation of its legacy internal IT infrastructure to identify and prioritize risks and vulnerabilities. Identified numerous weaknesses which could result in compromise of sensitive financial information. Provided recommendations for reducing cyber risk.

- Retained by an international financial institution to conduct a technical audit of their IT security systems. Conducted technical penetration testing and vulnerability assessments, reviewed security controls under FFIEC and NIST standards, and drafted a report summarizing findings and provided prioritized recommendations.

- Retained by a New York-based insurance company to conduct technical penetration testing and vulnerability assessments of its IT infrastructure. Identified numerous vulnerabilities and provided recommended remediations to comply with the New York Department of Financial Services' Cybersecurity Regulation.

- Conducted periodic cyber security assessments for a billion-dollar travel company, including technical penetration testing and vulnerability assessments and drafted reports summarizing the identified vulnerabilities and provided prioritized recommendations for remediation. Provided ongoing consulting services regarding internal cybersecurity initiatives, including interviewing and evaluating potential executive-level IT hires.

- Retained as an expert in a putative class action alleging a breach of a nationally recognized fast casual restaurant's payment systems was a result of negligent IT security practices. Reviewed documentation regarding the internal IT security architecture, policies, and procedures. Identified deficiencies and drafted demands for remediation.

- Retained by numerous clients across diverse industries, including legal services, real estate, financial services, and mining operations to conduct technical security assessments, including penetration testing, vulnerability scanning, and vulnerability remediation.

DIGITAL FORENSIC INVESTIGATIONS

- Provide ongoing investigative support to a US federal law enforcement agency regarding darknet investigations, including investigations into underground drug markets and ransomware command-and-control infrastructure.

- Retained by counsel for a popular resume-building website in connection with arbitration proceedings alleging that a competitor had stolen proprietary information from the website to enhance its own offerings. Analyzed website logs and databases from the claimant's website, as well as source code and GitHub repositories related to the development of the respondent's website and provided written expert testimony summarizing my findings.

DIGITAL FORENSIC INVESTIGATIONS (CONT'D)

- Retained by a foreign antivirus software developer to evaluate claims that its software presents unique information security risks to US government systems and networks. Conducted source code reviews, documentation reviews, and interviews to evaluate the functionality of the software and its potential security risks compared to other similar antivirus software.

- Retained as an expert by plaintiffs in a defamation lawsuit alleging the defendant made multiple defamatory postings about the plaintiff's business on an online medical provider reviews website and submitted a false report to a government regulator. Collected and analyzed forensic evidence and subpoena returns to construct a timeline of activity and conducted site visits to subject locations to verify findings.

- Retained by a foreign educational institution to investigate a data breach resulting in the leak of confidential documents to local newspapers. Collected and analyzed forensic evidence and conducted interviews to determine the source of the leak. Performed vulnerability testing to identify risks for additional data leaks and provided recommendations to improve security posture.

- Retained by a worldwide manufacturer of industrial power tools to investigate claims that an employee group had deployed unauthorized "shadow IT" infrastructure at an off-site location resulting in the potential disclosure of proprietary information. Conducted technical reconnaissance of the location and identified unauthorized wireless networks on company property.

- Retained by a New York-based law firm to investigate suspicions that its attorneys representing a high-profile client were being targeted by a spear phishing campaign intended to collect intelligence regarding an ongoing matter. Identified phishing emails targeted to the attorneys; extracted, reverse-engineered, and analyzed malware samples; and compiled a report regarding the analysis.

- Retained by a US-based mortgage lender to investigate the alleged unauthorized disclosure and use of sensitive credentials to access a restricted government database. Reconstructed and reviewed Oracle database logs and associated source code, interviewed US-based and India-based third-party software developers, and reviewed IT security policies and procedures. Drafted summary of investigative findings and provided recommendations for securely managing third-party database credentials.

- Retained as an expert by a well-known website which provides community-based classified ads as part of a civil suit against a competitor alleging the competitor was routinely scraping content from the plaintiff's website and reposting as their own. Analyzed web server logs to approximate the extent of the web scraping, evaluated its impact on the website's IT infrastructure, and provided recommendations to mitigate future web scraping activity.